Title : Code and Information Security

Author : Shigeo TSUJII et al.

(2) Memory Protection

This function permits an access to the data memory only when a predefined condition is met. The data memory is divided into multiple areas and different access conditions such as those listed in Table 10.2 are assigned on each of the areas. For example, an attempt to make a read/write access on an area where the condition 1 in the table is assigned is permitted only when the corresponding issuer key is verified positively through the process described in section (1) above. This means that the area is only accessible by the issuer. An attempt to make a read/write access on an area assigned with the condition 2 is permitted only when the corresponding user PIN is verified through the process described in the section (1), meaning that the area is only accessible by the user. Example data to be stored in each area is also listed in the table. Note that the description in the table is not of generic nature as the access condition specification largely depends on a specific application†.

(3) Security Function Using Encryption

This provides data encryption and authentication by using an encryption algorithm that is incorporated in the IC card.

† Access conditions are specified using an IC card issuing system. An optimal access condition supporting the use purpose can be selected by the IC card issuing system.

10. Information Security in the Social Life

Table 10.2 Example of access condition table

Issuer key has been verified		
User PIN has been verified		
PIN is not yet verified		
Example data		
	Read	Write
Condition 1	Encryption key	
Condition 2	Transaction data	
Condition 3	Account number, maximum credit amount	
Condition 4	User name	

10.1 IC Card and Security

Table 10.3 Advantages of IC card comprising display and keyboard(4)(7)

New functions

User identification can be carried out independently on the card

Data access can be carried out independently on the card

Added functions including a clock, calculator, and memo pad

Benefit for the card user

The time required for credit inquiry etc. is reduced

Data (for example, credit balance and transaction detail) contained in the card can be accessed without using a terminal device

Increased added values

Benefit for the card issuer

Communication costs are saved

Table 10.4 Subject areas concerning IC card standardization discussed by ISO(8)

Elements to be standardized	Key agendas	Status
1 IC card definition and physical properties		
2 Dimension and position of external terminals		
3 Electrical signal and exchange protocol		
4 Common set of commands for the IC card		
5 Massage format		
6 Logical configuration of on-card memories		
7 Card life cycle		
8 Transaction process		
9 Key management		

Definition of the IC card with an external terminal; standards for

an environmental resistance test, etc.

Position, dimension, and signal assignment etc., of the external terminals

Built-in IC electrical properties (NMOS/CMOS-based); method for providing control signals; communication protocol for exchanging information (character transmission/block transmission system)

Basic functions common to different applications (related with items 5 and 6)

Message configuration between the IC card and equipment (transaction settlement messages in the financial sector)

Memory access method (physical address/logical address); access right control system, etc.

Security management involved with different stages in the IC card life cycle including manufacture, issuance, use, and decommission.

Transaction procedure using IC cards; prevention of illegal transactions (for example, user identification and various types of authentication)

Management of the control information (for example encryption key and PIN) required for implementing items 7 and 8

Established1)3)

Established2)3)

Notes:

1 to 4: Standardization of the IC card itself (responsible committee: ISO/IEC, JTC1/SC17WG4)

5 to 9: Standardization of application systems for the financial sector (responsible committee: ISO TC68/SC6/WG5, 7)

DIS: Draft International Standards

10.1.4 IC Card Security Technologies in the Future

Keeping in mind a possible advance of the IC card in the future, security functions that are optimized for the IC card have been actively proposed recently. Some of them are outlined below.

In one aspect, the IC card is assumed as a physically secure device or as a TFM (Tamper Free Module), and based on this assumption, efforts are made to implement necessary functions in a simple manner that would otherwise add up to a complicated mechanism in most cases. For example, a digital signature, that is generally considered difficult to be implemented without the aid of public key cryptogram, can easily be implemented in combination with common key cryptogram if the IC card per se is supposed to be secure physically. An example implementation (9) is as follows. First, following assumptions are made.

1) The same encryption key K is used for all IC cards. Different ID numbers are used for each of the IC cards.

2) The IC card issuer writes the encryption key and ID number into respective IC cards.

3) Access protection is provided for the encryption key using the condition 1 listed in Table 10.2 as well as for the ID number using the condition 3.

4) The issuer is trustworthy.

As shown in Fig. 10.4, when user A sends a message M with

his signature to user B, the user A enters his PIN on the IC card A and then instructs the card A to place the signature on the message M. As the PIN has already been verified, the card A accepts the instruction to initiate a signature process. The card A adds its own ID number IDA at the tail of M, carries out encryption with EK, and returns the encryption output C to the user A. The user A sends C to the user B. The user B instructs the IC card B to decrypt C. The card B decrypts C with DK to return the result to the user B. The user B checks to confirm the user A's ID number IDA attached to the tail of M. Needless to say, this ID number represents the user A's signature.

The security in the use of this system is discussed below. First, forgery of the user A's signature cannot be achieved on any cards other than the IC card A. Any attempt to forge the "signature" on other IC card is immediately detected from the ID number of that particular card that is appended automatically when the signature is placed using that card. No one but the issuer who is trustworthy can rewrite the ID number as it resides in the area where the condition 3 is assigned. Furthermore, forgery of the signature using the decryption instruction is not possible for reasons as follows. The signature of the user A must be in the format EK (M, IDA). If it is possible to find M' that satisfies

$$DK(M')=EK(M, IDA)$$

or

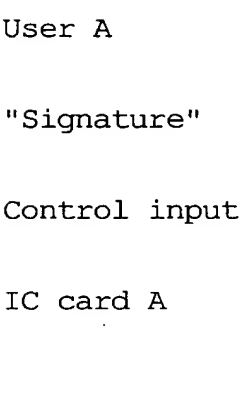
M'=EK(EK M, IDA)),

a forged signature can be obtained by decrypting M', however, it is difficult to solve the equations shown above. Furthermore, only the user A can use the IC card A because the card performs PIN verification. In other words, signature text C can be produced only when the user A uses his own IC card. It is the digital signature technology that enables this functionality.

Public key cryptogram can also be configured with common key cryptogram if one assumes that the IC card is TFM(10). Fig. 10.5 depicts this configuration. In Fig. 10.5, (E, D) and (E', D') represent a pair of encryption and decryption, respectively of the common key cryptogram. A procedure during the card issuance is described first. A trustworthy issuer writes a secret key KI that is common to the entire system and a secret key KSB specific to the IC card B into the memory of the IC card B where access protection is implemented. The issuer then encrypts the secret key KSB with E'KI to disclose it as a public key KPB for the user B. The same procedure applies to other IC cards. A process involved with the use of cards is described next, supposing that the user A conducts a secret communication with the user B. The user A enters a message M and the public key KPB of the user B in user A's IC card and issues an encryption instruction. The IC card decrypts KPB with D'KI, internally obtains the user B's secret key KSB to use it as a key to encrypt M with EKSB, and returns the output C to the user A. The user A in turn sends C to the user B. The user B enters his

PIN into his IC card and then gives an instruction to decrypt C. The IC card uses the secret key KSB stored therein to decrypt C with DKSB and returns the message M to the user B.

Fig. 10.4 Digital signature based on physical security



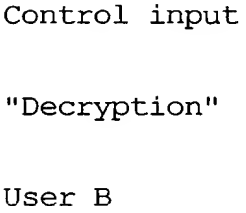
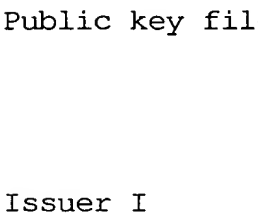


Fig. 10.5 Public key cryptography based on physical security



User A

"Encryption"

Control input

IC card A

Control input

IC card B

"Decryption"

User B

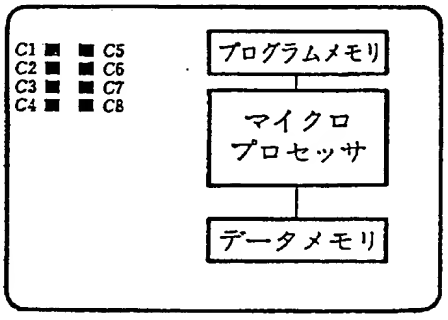
【受入日】 19971022
【情報館受入日】
【ＣＳターム】 EE03、EZ04、GZ01、GZ03、JZ08、KZ60、LL03
【フリーワード】 ネットワーク社会、整数論、有限体理論、慣用暗号、Ｆｅｉｓｔｅｌ暗号、ＤＥＳ暗号、ＦＥＡＵ暗号、暗号文ランダム性評価指標、公開鍵暗号、ナップザック問題、多変数非線形連立方程式、確率的暗号、擬似乱数、ＩＤ認証付鍵配送方式、符号理論、線形符号、巡回符号、ＢＣＨ符号、Ｇｏｐｐａ符号、ディジタル署名、零知識会話型証明、情報セキュリティ、暗号化鍵配送法、データ回線暗号装置、ストリーム暗号、スクランブル放送、スクランブル技術、ＰＮ系列発生器、アクセスコントロール、ファイル暗号化、復号化、セキュリティコントロール、ＩＣカード、電子金融システム、放送業
【許諾レベル】 1Z
【著者群】
【著者名】 辻井 重男
【著者所属】 東京工業大学
【共同著者名】 笠原 正雄
【共同著者所属】 京都工芸繊維大学
【共同著者名】 宮口 庄司
【共同著者所属】 日本電信電話株式会社
【共同著者名】 黒澤 馨
【共同著者所属】 東京工業大学
【共同著者名】 田中 初一
【共同著者所属】 神戸大学
【共同著者名】 中村 勝洋
【共同著者所属】 日本電気株式会社
【共同著者名】 難破 誠一
【共同著者所属】 日本放送協会
【共同著者名】 上園 忠弘
【共同著者所属】 日本アイ・ビー・エム株式会社
【共同著者名】 神竹 孝至
【共同著者所属】 株式会社東芝
【論文タイトル】
【資料タイプ】 単行本
【ブックＩＤ】
【書籍タイトル】 暗号と情報セキュリティ
【編集者名】 辻井 重男 SHIGEO TSUJI
【編集者所属】 東京工業大学
【編集者名】 笠原 正雄 MASAO KASAHARA
【編集者所属】 京都工芸繊維大学
【発行者名】 株式会社昭晃堂
【開催日・発行日】 19900329
第1版 ISBN: 4-7856-3075-2
【頁】 1～245

技術が盛んに提案されている．これらは，第2～3章の基礎暗号技術や，10.1のICカードの応用である．これらの議論は，始まったばかりであり，将来どのような形で実現されるのか必ずしも明確ではないが現在の状況を10.2で説明しよう．

10.1 ICカードとセキュリティ

10.1.1 ICカードとは何か

物理的には，ICカードは現行の磁気ストライプ付クレジットカードと同サイズのカード基板（54×86×0.76mm）中にICを内蔵し，カード面にICの外部端子を有するIDカードと定義できる[(1)(3)]．図10.1はICカードの構成を示したものである．IC部は，マイクロプロセッサを中心に，プログラムメモリ，データメモリが接続された構成である．バッテリは通常カードの中には埋め込まれていない†ので，ICカード単体では動作しない．ICカードを動作させるには，専用のアダプタ（リーダライタという）が必要である．ICカードとリーダライタの入出力は，カード表面に形成された8つの外部端子を用いて電気的に行う．リーダライタは，ICカードが挿入されると，外部端子上に電極を降ろし，電源，クロックを与えてプロセッサを活性化した後，情報のやり取りをする．なお，ICカードをリーダライタから取り出したとき（すなわちICカード



（a） 構成例

図10.1 ICカードの構成

番号	端子記号	端子名	端子の機能
1	C1	VCC	回路電圧（V_{cc}）
2	C2	RST	リセット信号
3	C3	CLK	クロック信号
4	C4	RFU	将来のための予備端子（現在は，使用できない）
5	C5	GND	ゼロ電圧
6	C6	VPP	プログラム供給電圧（V_{pp}）
7	C7	I/O	データ入出力
8	C8	RFU	将来のための予備端子（現在は，使用できない）

（b） 端子の割付け[(2)(3)]

† バッテリのついたICカードも最近登場している．これについては，10.1.2で説明する．

に電源が供給されないとき），データメモリの内容が消去されないよう，データメモリは不揮発性メモリ†で構成される．

ICカードの特徴は，磁気カードと比較すると分かりやすい．磁気カードの問題点は低記憶容量（10^2～10^3ビット）とデータに対する保護がないこと††である．一方，ICカードは磁気カードの100倍以上の記憶容量を持ち(4)，さらに処理能力も持つ．この処理能力を用いて記憶データの保護などセキュリティ機能が実現できるのである．この大記憶容量と処理機能(特にセキュリティ機能)を生かして，ICカードは金融分野ほか表10.1の分野に使われようとしている．

以下ではICカードで実現できるセキュリティ機能の概略を説明する．本書では，セキュリティ機能のみ説明するが，ICカードの機能はこれに限定したものではないことを注意しておく．

10.1.2　現行ICカードのセキュリティ機能

ICカードで現在実現されているセキュリティ機能は，次の3つである．

（1）　PINを用いた本人確認機能

ICカードを使用しようとしている人が正当な持ち主であることを，暗証番号(Personal Identification Number, PIN) を用いてICカード自身が確認する機能である．確認手続きはおおよそ，次のようになる(5)(6)．ユーザがリーダライタに付属のキーボードを用いてICカードにPINを入力すると，ICカードはこれをあらかじめ記憶していたPINと照合する．こうして得られた照合結果は，それ以降のメモリアクセス，コマンド実行の際参照され，アクセス／実行の可否判定に使用される．なおアプリケーションによっては，一定の回数の間に正しいPINが入力されないと，ICカードは現在のユーザが正当なユーザではな

† PROM, EEPROMなど．PROMの場合，データメモリの内容は消去できない．したがってICカードは使い捨てになる．EEPROMの場合，メモリの消去が可能なので，ICカードは繰り返し使える．

†† 磁気カードの記憶データは，市販のリーダライタで簡単に読める．したがってPINなど秘密の情報を磁気カード内に記憶させるのは危険である．なお最近の銀行用カードでは，PIN照合をセンタで行う方式が全面的に採用されている．

表 10.1 ICカードの応用分野

応用分野	用途例
金融	キャッシュカード，クレジットカード，証券・証書カード
流通	商品券，ショッピングカード，友の会カード
交通	定期券，回数券，有料道路通行券，駐車場カード
医療	診察券カード，健康保険証カード，電子カルテ
OA	端末操作カード，データファイルカード，プログラムカード
FA	NCカード，工場管理カード
HA	電話カード，ホームコントロールカード，調理メニューカード
セキュリティ機能	身分証明カード，会員カード，入退室管理カード，オペレーションカード
レジャー他	電子メイル，図書貸出券，メンバカード

OA: Office Automation
FA: Factory Automation
HA: Home Automation
NC: Numerical Control (数値制御)

いと判断し，自分自身をロック（以降のアクセスを禁止）する．

（2） メモリ保護機能

あらかじめ決められた条件に合致したときのみ，データメモリへのアクセスを許可する機能である．データメモリは，複数の領域に分割され，各領域にはたとえば表10.2のようなアクセス条件が設定される．表において，たとえば条件1の領域は，発行者キーを（1）の手順を用いて確認した後，初めて読み書きが許される領域である．言い換えれば，この領域は発行者のみがアクセスできる領域である．また条件2の領域はユーザPINを（1）の手順を用いて確認した後，初めて読み書きが許される領域である．言い換えれば，この領域はユーザのみがアクセスできる領域である．それぞれの領域に蓄えられるデータの例は表の通りである．アクセス条件の設定は，アプリケーションによってかなり異なる†．表が，必ずしも一般的とはいえないことに注意されたい．

（3） 暗号化を用いたセキュリティ機能

ICカード内に暗号化アルゴリズムを入れ，これを使ってデータの暗号化，認証を行う機能である．

† アクセス条件の設定はICカード発行システムを用いて行う．ICカード発行システムによって，利用目的に最適のアクセス条件を選ぶことができる．

表 10.2　アクセス条件テーブルの1例

	発行者キーの確認後		ユーザPINの確認後		PINの確認以前		データ例
	リード	ライト	リード	ライト	リード	ライト	
条件1	○	○	×	×	×	×	暗号化鍵
条件2	×	×	○	○	×	×	取引きデータ
条件3	○	○	○	×	×	×	口座番号，与信限度額
条件4	○	○	○	×	○	×	氏名

以上説明した基本セキュリティ機能が実システムの中でどう使われるか，フランスのPOS(Point-of-Sale)†実験システムの例で示しておこう[5]．買い物を行うとき，ユーザはまずICカードをPOS端末に挿入する．店員が入力した金額に間違いがなければ，ユーザはユーザ専用のキーボードからPINを入力する．このPINがICカード内のPINと一致し（機能(1)）さらにPOS端末が店員のICカードによって活性化されていれば，端末はICカードに今月の買い物リストと月当りの限度額を読み出す命令を与える．ICカードは，PINを確認ずみなのでこの命令を受け入れ，リストと限度額を出力する（機能(2)）．端末はリストの合計額と今回の額を加算し，限度額と比較する．限度額以内であれば買い物が許可され，端末は日時，今回の金額を書き込む命令をICカードに与える．ICカードは，PIN確認ずみなのでこの命令を受け入れ，前回までのリストに今回のデータを付け加え（機能(2)），支払い手続きが終了する．この例では，ICカード内の買い物データの読み出し，更新は，ユーザPINと正規のPOS端末の両方が揃わないとできない．これによりICカード内のデータの信頼性を高めているのである．

次に，フランスのホームバンキング・システム††（テレペイメントシステムと呼ばれている）の例を示す．手順は図10.2に示す通りである[5][6]．

① ユーザがPINを入力する．

② ICカードはこれをカード内のPINと比較する（機能(1)）．

† POSシステムは，小売り販売に必要な様々な手続きを自動化したシステムである．ここでは特に，ICカードを用いて支払いを自動化することを意味している．

†† 自宅，会社の端末と金融機関のコンピュータを通信回線で結び，取引きを行ったり，サービスを受けることを可能としたシステム．

③ ユーザの口座番号が銀行のコンピュータ（以下，銀行と略す）に送信される．

④ 銀行は乱数を生成し，カードに送信する．

⑤ 端末がICカードに認証子を生成するよう命令する．ICカードは，PIN照合ずみなのでこの命令を受け入れ，暗号化鍵，口座番号，乱数の3つからあるアルゴリズムを用いて認証子を生成する（機能（3））．一方，銀行も同一のアルゴリズムにより，認証子を生成する．

⑥ ICカードで計算された認証子が銀行に送信される．

⑦ 銀行は両者の認証子を比較する．

⑧ 同一であれば，銀行は通信相手が確かに送信された口座番号のユーザと分かるので，取り引きを許可する．

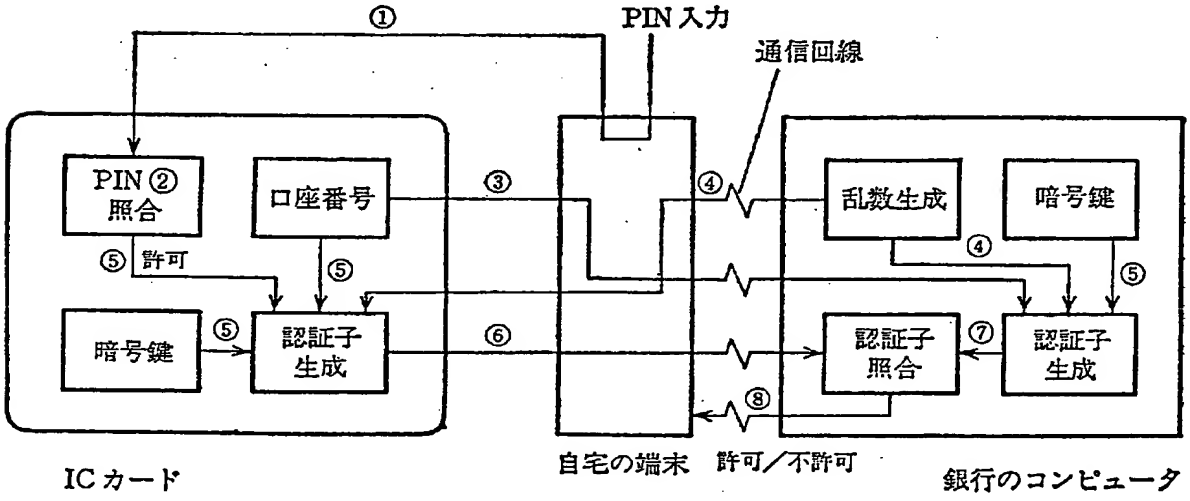


図 10.2 テレペイメントシステム（フランス）の例[5]

また我国の全銀協標準仕様案では，多目的利用を目標とし，1枚のICカードに複数のアプリケーションが登録できるようになっている．この際，アプリケーション相互間のセキュリティを確保することが重要であるが，ここでも（1）のPIN照合機能と（2）のメモリ保護機能が重要な役割を果たしている．

最後に，最近登場してきたディスプレイ，キーボード付のICカード（図

10.3参照）について簡単に述べる．これは，単独での使用を可能にするため電源も内蔵している．表10.3はディスプレイ，キーボード付のICカードの利点を示したものである．表中，特にセキュリティとかかわる事項は，このカードはカード単体で本人確認や内部データへのアクセスができるので，さらに安全な点である．運用方法によっては端末なし，すなわちオフラインで安全な取引きを行うことも可能である．

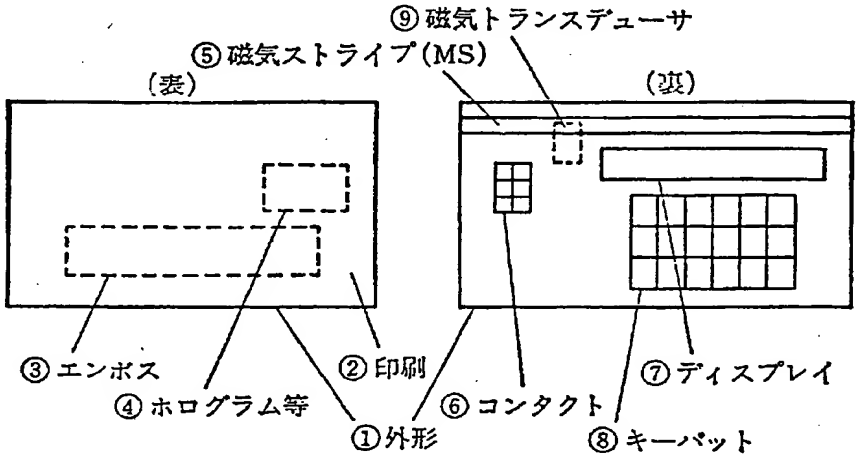


図 10.3　ディスプレイ，キーボード付ICカード[4] (MS: Magnetic Stripe)

10.1.3　標準化動向

国際標準化機構 (International Organization for Standardization, ISO) のJTCI/SC17およびSC68/SC6委員会で，ICカードの標準化作業が進められている．標準化項目とそれぞれの項目の1988年までの進行状況は表10.4の通りである[8]．物理特性，外部端子の寸法，位置に関しては，ISO標準がすでにできている．電気信号および交換プロトコルについてはISO標準案が決まった段階である．セキュリティに関連のある④～⑨については，これから議論が加速されることになろう．

表 10.3 ディスプレイ，キーボード付ICカードの利点[4][7]

新しく加わった機能	カード利用者の利点	カード発行者の利点
カード単独で本人確認が可能	信用照会などにかかる時間が短縮される	通信コストを低減できる
カード単体でデータアクセス可能	カード内データ（与信残高，取引明細など）を端末なしにアクセスできる	通信コストを低減できる
時計・電卓・メモ帳などの付加機能	付加価値を高められる	

表 10.4 ISOにおけるICカード標準化審議項目[8]

	標準化項目	主要審議事項	進行状況
①	ICカードの定義と物理特性	外部端子付ICカードの定義，耐環境性テストの規格等	制定済[1][3]
②	外部端子の寸法および位置	外部端子の位置，寸法，信号の割付け等	制定済[2][3]
③	電気信号および交換プロトコル	内蔵ICの電気特性（NMOS/CMOS対応），制御信号供給方法，情報交換のための通信規約（キャラクタ伝送／ブロック伝送方式）	DIS
④	ICカードの共通コマンド	各種応用分野に共通の基本機能（⑤⑥と関連）	
⑤	メッセージフォーマット	ICカードと装置間の電文の構成（金融分野の決済用メッセージ）	
⑥	カード内メモリの論理的構成	メモリへのアクセス方法（物理アドレス／論理アドレス指定方式），アクセス権制御方式等	
⑦	カードのライフサイクル	ICカードの製造，発行，運用，廃止等の各段階でのセキュリティ管理	
⑧	トランザクションプロセス	ICカードによる取引き手順，不正取引きの防止（本人確認，各種認証等）	
⑨	キーマネージメント	⑦⑧の実現に必要な制御情報（暗号化鍵，暗証番号等）の管理方法	

（注） 上記①～④：ICカード自体の標準化（担当委員会：ISO/IEC JTC1/SC17/WG4）
上記⑤～⑨：金融分野用利用システムの標準化（担当委員会：ISO TC68/SC6/WG5, 7）
DIS：Draft International Standards（国際標準案）

10.1.4 将来のICカードのセキュリティ技術

将来のICカードの進歩を見越して，最近ICカードに適したセキュリティ機能の提案が盛んに行われている．ここではその幾つかを紹介する．

1つの考え方は，ICカードを物理的に安全な装置，すなわち**TFM** (Tamper Free Module) とみなして，一般には複雑な仕掛けになりがちな機能を簡易に

実現しようというものである．たとえば，ディジタル署名は，通常公開鍵暗号を使わなければ実現困難だが，ICカードが物理的に安全であれば，ICカードと共通鍵暗号を組み合わせて，容易に実現できる．以下実現例[9]を説明しよう．まず以下の仮定を置く．

① 暗号化鍵KはすべてのICカードに共通．ID番号はそれぞれのICカードごとに異なる．

② ICカードの発行者は暗号化鍵とID番号をそれぞれのICカードに書き込む．

③ 暗号化鍵は表10.2の条件1，ID番号は条件3のアクセス保護がされている．

④ 発行者は信用できる．

ユーザAがユーザBにメッセージMを署名付きで送信する場合，図10.4の

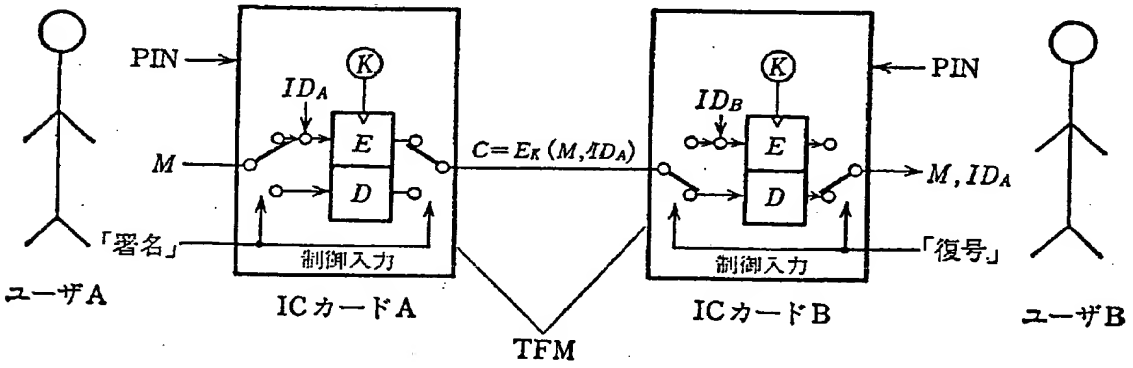


図 10.4　物理的安全性に基づくディジタル署名

ようにユーザAは自分のICカードAにPINを入力し，ついでMに対し署名を行うようカードAに命令する．カードAはPIN照合ずみなのでこの命令を受け入れ，署名プロセスを起動する．カードAはMの終わりに自己のID番号ID_Aを付け加え，E_Kで暗号化した後，暗号出力CをユーザAに渡す．ユーザAはCをユーザBに送信する．ユーザBはICカードBにCを復号するよう命令する．カードBはCをD_Kで復号し，復号結果をユーザBに渡す．ユーザBはMの後に，ユーザAのID番号ID_Aがついていることを確認する．いうまでも

なく，このID番号がユーザAの署名に相当する．

次にこのシステムの安全性について考えてみよう．まず，ICカードA以外のカードでは，ユーザAの署名を偽造することはできない．他のICカードで「署名」を行うとそのカードのID番号が自動的につくので偽造がただちに検出できるからである．ID番号は条件3の領域にあるので信用できる発行者以外書替えは不可能である．また，「復号」命令を悪用して署名を偽造することも次の理由により不可能である．ユーザAの署名は$E_K(M, ID_A)$の形式をしていなければならない．もし，

$$D_K(M')=E_K(M, ID_A)$$

あるいは，

$$M'=E_K(E_K(M, ID_A))$$

をみたすM'を発見できれば，このM'を「復号」することにより，署名の偽造ができるが，上記方程式を解くのは困難だからである．さらにICカードAは，PIN照合を行うので，ユーザA本人しか使えない．つまり署名文CはユーザAがユーザAのICカードを使わなければ作れない．これは，ディジタル署名の機能にほかならない．

ICカードをTFMとみなせば，さらに公開鍵暗号も共通鍵暗号で構成できる[10]．図10.5がその構成図である．図中(E, D) (E', D')は各々共通鍵暗号の暗号化，復号の対を表す．まず発行時の手順を説明する．信用できる発行者は，システム全体に共通の秘密鍵K_IとICカードB固有の秘密鍵K_{SB}を，ICカードB内のアクセス保護がされているメモリに書き込む．さらに，発行者は，秘密鍵K_{SB}をE'_{KI}で暗号化し，これをユーザB用の公開鍵K_{PB}として公開する．他のICカードについても同様な手続きを行う．次に運用時の手順を，ユーザAがユーザBに秘密通信する場合で説明する．ユーザAは，メーセージMとユーザBの公開鍵K_{PB}をICカードに入力し，暗号化命令を与える．ICカドは，K_{PB}をD'_{KI}で復号化しユーザBの秘密鍵K_{SB}を内部的に得，これを鍵としてMをE_{KSB}で暗号化し，出力CをユーザAに返す．次にユーザAはCをユーザBに送信する．ユーザBはPINを自分のICカードに入力した後，Cを

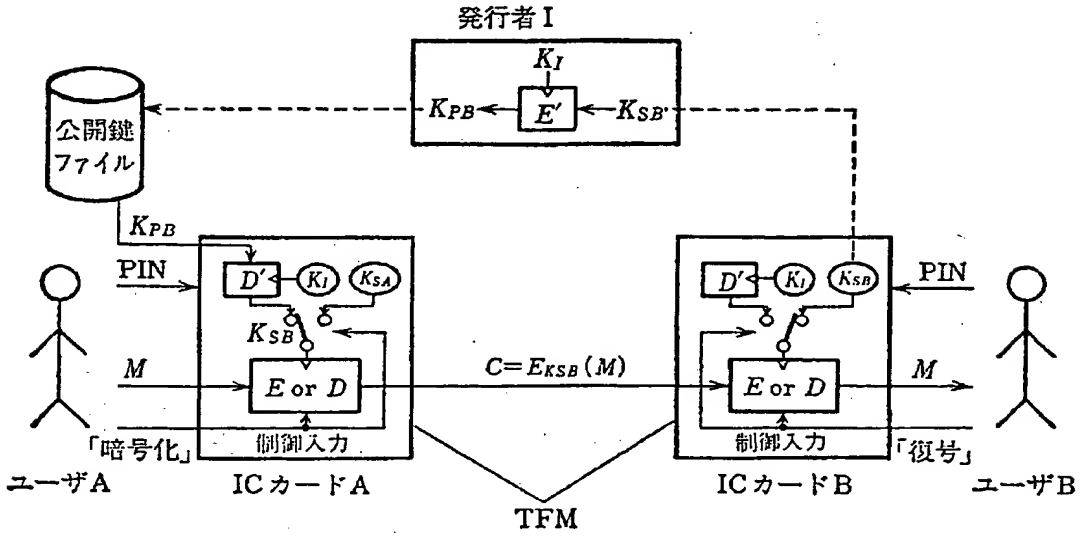


図 10.5　物理的安全性に基づく公開鍵暗号

復号する命令を与える．ICカードは内部に記憶している秘密鍵K_{SB}を用いCをD_{KSB}で復号し，メッセージMをユーザBに返す．

この方式のキーポイントは「暗号化命令」と「復号命令」の時で，鍵が自動的に切り替わることである．ユーザBへの暗号化は，外部から公開鍵K_{PB}を入力することによってどのカードでもできるが，復号は秘密鍵を内部に記憶しているカードB以外できない．ディジタル署名もこのシステムを使って容易に実現できる．その時には，「暗号化命令」と「復号命令」を逆に使えば良い．また図10.5と同様な構成でIDに基づくシステムも実現できる．詳細は文献(11)を参照されたい．

パリに本部のある**国際ICカード協会** (International Association for Microcircuit Card, INTAMIC) はRSA暗号のICカードへの応用を検討している．以下，このICカードを用いたPOSの手順案を示す（図10.6参照）．なお，記号の説明は文章中で行うと繁雑なので，図10.6にまとめて示した．

① ユーザがPINを入力すると，ICカードはそれを照合する．

② 端末はICカードに，KITを通知する．なおKITは発行者によって端末内のメモリにあらかじめ書き込まれている．ICカードはKITを鍵K_{PI}

ID_C=カードID
ID_T=端末ID
R=乱数
TD=取引きデータ
(K_{PI}, K_{SI})=発行者の公開鍵および秘密鍵
(K_{PC}, K_{SC})=カードの公開鍵および秘密鍵
(K_{PT}, K_{ST})=端末の公開鍵および秘密鍵
○=当初から保有する鍵
△=計算で得た鍵
D=RSA暗号の復号
$KIC=D_{KSI}(ID_C, K_{PC})$
　カードIDおよびカードの公開鍵に発行者秘密鍵で署名したもの
$KIT=D_{KSI}(ID_T, K_{PT})$
　端末IDおよび端末の公開鍵に発行者秘密鍵で署名したもの

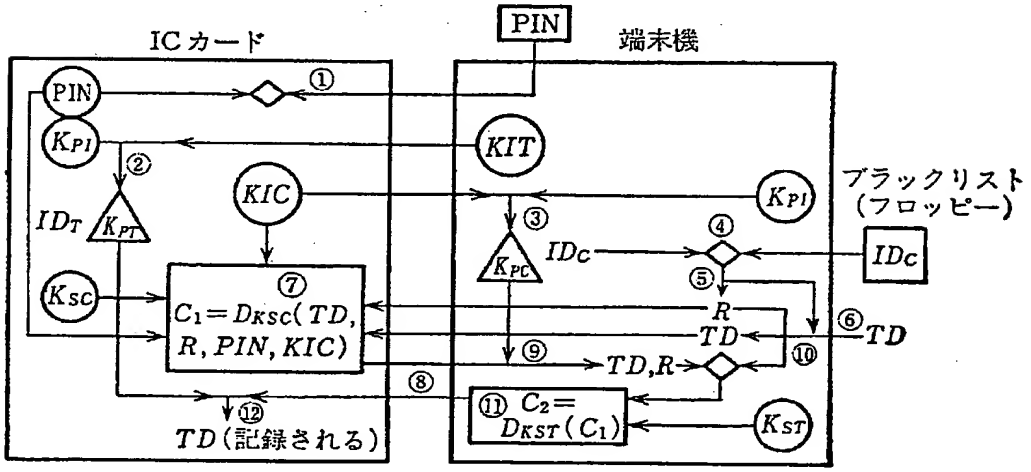


図 10.6 INTAMICのICカードシステム構想[12]

で暗号化 E_{KPI} し ID_T, K_{PT} を得る.

③ ICカードは端末に KIC を出力する. なお KIC は発行者によってICカード内のメモリにあらかじめ書き込まれている. 端末は KIC を鍵 K_{PI} で暗号化 E_{KPI} し ID_C, K_{PC} を得る.

④ 端末は ID_C が, 使用停止のカードリストに載っていないことを確認する.

⑤ 端末は乱数 R をカードに送る.

⑥ 端末は取引きデータ TD をカードに送る.

⑦ カードは鍵 K_{SC} を用いて署名文 C_1 を作る.

⑧ カードは C_1 を端末に出力する.

⑨ 端末は③の手順で得たK_{PC}を使ってC_1を暗号化E_{KPC}する.

⑩ その結果得られたTD, Rが元のTD, Rと一致することを確認する.

⑪ 端末はC_1をK_{ST}で署名し，その結果$C_2=D_{KST}(C_1)$をカードに送る.

⑫ カードはC_2を②の手順で得たK_{PT}で暗号化E_{KPT}し，結果が元のC_1と一致することを確認する. ICカードはTDを記録し取り引き手順が終了する.

本方式では，カードと端末間の正当性確認のためにRSA暗号が使われている. たとえば，端末はカードに電文R, TDを送り，カードの秘密鍵K_{SC}で署名させている. 端末はこれをカードの公開鍵K_{PC}で暗号化し，電文R, TDが得られることを確認することにより，カードの正当性確認を行っている†.

本方式の特徴は，公開鍵K_{PC}を得る方法にある. RSA暗号システムの基本形態では，各端末が公開鍵ファイルを持つ. しかし，実際に各端末に公開鍵ファイルを置くのはメモリ容量，管理の点から非常に難しい. そこでここでは，端末は必要のつどカードから公開鍵K_{PC}を受け取る構成をとっている. ただし，カードからK_{PC}を受け取る構成では，秘密鍵K_{SC}と公開鍵K_{PC}の両方をねつ造することによるカード偽造が可能になり，せっかくの正当性確認が無意味になる心配がある. これを防止するために，カードはK_{PC}そのものではなく，K_{PC}を発行者の秘密鍵K_{SI}で署名したKICを記憶しているのである. 発行者以外K_{SI}を知らないので，K_{SC}とKICを対応するよう書き替えることは困難である. これにより安全性が保てる. 各端末は発行者の公開鍵K_{PI}だけを持てば良い. このような公開鍵の管理方法は，Daviesも提案している(13).

RSA暗号など公開鍵暗号をICカードに実装するときの1つの問題点は，ICカードの計算能力不足と予想される. この問題に対して，最近，「ICカードのように計算能力が限られたマシンが外部のよりパワフルな装置の計算能力を借りて計算（暗号化，復号）を行いつつ，自分の所持する秘密（平文，秘密鍵）は外部に漏らさないにはどうすれば良いか」という検討がされている. この詳細については文献（14）を参照されたい.

† ICカードが端末の正当性を確認するときも同様な方式が使われている.

暗号と情報セキュリティ

中央大学教授／工学博士
辻井　重男
京都工芸繊維大学教授／工学博士
笠原　正雄
編著

株式会社 昭晃堂

1990年3月29日　初版1刷発行
1992年5月20日　初版2刷発行
1994年4月30日　初版3刷発行
1996年2月20日　初版4刷発行

編集者紹介
辻井重男（つじいしげお）　工学博士
昭和33年　東京工業大学電気工学科卒
現　在　東京工業大学工学部名誉教授
中央大学教授

笠原正雄（かさはらまさお）　工学博士
昭和40年　大阪大学大学院博士課程終了
現　在　京都工芸繊維大学教授

検印省略
著者承認

暗号と情報セキュリティ
(Cryptography and Information Security)

© 編著者　辻井重男
笠原正雄
発行者　阿井國昭
東京都新宿区矢来町48
印刷所　大和印刷
東京都新宿区改代町24
発行所　株式会社 昭晃堂
郵便番号 162　東京都新宿区矢来町48
振替口座　00130-0-139320
電話(03) 3269-3449(代表)
FAX(03) 3269-1611

定価はカバーに
表示してあります

Printed in Japan
日本書籍出版協会会員
自然科学書協会会員
工学書協会会員

製本　小林共文堂

ISBN4-7856-3075-2